As of: November 2026

SPECIALIST MANUAL

HAZARD ALERT TECHNOLOGY & SECURITY SERVICES

Alarm Monitoring of Hazard Alert Systems

Alarm Response and Preventive Security

SPECIALIST PORTALS AND BRANDS OF SECUCONCEPT

Standards & technology: DIN VDE 0833 · DIN EN 50131 · DIN EN 50136 · DIN EN 50518

Alarm response in accordance with DIN 77200-1 · Rights and limits during deployment

Client cooperation · Prevention · Cost examples · Checklists

Quality through Trust

SecuConCept · Security – Consulting – Conception · www.secuconcept.de

0800 666 000 4 · vertrieb@secuconcept.de

ABOUT THIS MANUAL

An Alarm Is Only the Beginning

A hazard alert system protects only as well as the chain that takes over after the alarm: secure transmission, a permanently staffed alarm receiving centre, a clear alarm plan, a fast and legally sound intervention – and a client whose employees know what to do when an incident occurs. If one link is missing, the alarm remains without consequence or turns into an expensive false alarm.

This manual is intended for executive management, facility and security management, technical managers, procurement, and branch and site managers in industry, logistics, retail, public administration and critical infrastructure. It brings together standards, procedures, rights and obligations, client cooperation, prevention and cost examples in a single document.

Contents

1 At a Glance 3

2 Hazard Alert Systems and Alarm Monitoring 4

3 Alarm Receiving Centre and Alarm Response 7

4 Client Cooperation 10

5 Preventive Security 12

6 Law, Liability and Data Protection 13

7 Cost Examples and Cost-Effectiveness 14

8 Checklist for Clients 16

9 Frequently Asked Questions (FAQ) 17

10 Your Partner for Alarm Monitoring and Intervention 18

11 Sources, Standards and Legal Status 19

KEY MESSAGES FOR DECISION-MAKERS

01 At a Glance

The ten most important facts for operators who want to connect hazard alert systems to an alarm receiving centre, commission alarm response services or improve their prevention.

1 **The standards framework is clear:** DIN VDE 0833 (hazard alert systems), DIN EN 50131 (intruder and hold-up alarm systems, Grades 1–4), DIN EN 50136 (alarm transmission), DIN EN 50518 (alarm receiving centre).

2 **Grade and class define the system:** The police recommend Grades 2 to 4 for intruder alarm systems; insurers frequently require VdS-approved systems of Classes A, B or C.

3 **Fire alarm systems connected to the fire service** are routed via the alarm transmission network of the local concession holder in accordance with DIN 14675 – not via a private alarm receiving centre.

4 **Transmission paths age:** The 2G networks will be switched off from 2028 onwards. Alarm transmission devices whose only backup path is GSM must be upgraded in good time.

5 **Alarm response is an intervention service under DIN 77200-1:** agreed measures in response to a non-regular event within a defined period.

6 **Security staff have no police powers:** They act on the basis of delegated domiciliary rights (Hausrecht) and the so-called everyman's rights – and without special privileges in road traffic.

7 **Nothing works without the client's cooperation:** An up-to-date alarm plan, reachable contact persons and trained employees are the most effective measures against false alarms.

8 **False alarms cost money:** Depending on the federal state, fees may be charged for police deployments; courts have confirmed, for example, 120 € per unjustified alarm call-out.

9 **Prevention first:** Mechanical resistance, organisation and visible patrols prevent offences – detection and intervention technology limits the damage.

10 **Insurance cover depends on policyholder obligations:** Anyone who fails to arm an intruder alarm system agreed in the policy risks a reduction of benefits (§ 28 VVG, German Insurance Contract Act).

Important note on legal validity

This manual provides professional guidance and is no substitute for legal advice. Standards, guidelines, the connection requirements of fire services and police, and the fee schedules of the federal states change over time and differ from region to region. Research status: November 2026. All cost figures are non-binding reference values (net) and do not replace a site-specific quotation.

SYSTEM TYPES · GRADES AND CLASSES · CONNECTION TARGETS · TRANSMISSION

02 Hazard Alert Systems and Alarm Monitoring

Hazard alert systems (GMA) detect intrusion, hold-up, fire or technical faults and report them to a permanently staffed centre. Which centre that is, and which requirements apply, depends on the type of alarm.

2.1 System types at a glance

System type	Typical alarms	Relevant standards and rules
Intruder alarm system (EMA)	Opening, break-through, movement, glass breakage, tampering	DIN EN 50131, DIN VDE 0833-1/-3, VdS 2311
Hold-up alarm system (ÜMA)	Silent alarm, threat, personal distress signal	DIN EN 50131, DIN VDE 0833-3, ÜEA Guideline
Fire alarm system (BMA)	Smoke, heat, manual call points, extinguishing system activation	DIN EN 54, DIN VDE 0833-2, DIN 14675
Technical alarms	Temperature, water, power failure, refrigeration, gas	Manufacturer specifications, site-specific definition
Video and perimeter alarms	Fence detection, video analytics, tampering	DIN EN 62676, see the Video Surveillance Manual

2.2 Grades under DIN EN 50131 and VdS classes

The DIN EN 50131 series divides intruder and hold-up alarm systems into four grades. In Germany, DIN VDE 0833-1 and -3 supplement the series; for systems relevant to insurance cover, the VdS 2311 guideline with Classes A to C additionally applies.

Grade	Risk / field of application	VdS class (approx.)	Note
Grade 1	low risk	–	not recommended by the police
Grade 2	low to medium risk, residential, small businesses	Class A	minimum standard for alarm monitoring
Grade 3	medium to high risk, commercial premises, warehouses	Class B	frequent insurance requirement
Grade 4	high risk, banks, high-value storage, special facilities	Class C	inspection four times a year

The mapping of grades to VdS classes is an approximation; the insurance contract, the installer's certificate and the individual system design are decisive.

2.3 Where is the system connected to?

Target	For which alarms	Requirements
Private alarm receiving centre (ARC)	Intrusion, hold-up, technical alarms, video, faults, arming/disarming monitoring	Contract, alarm plan, key holding; ARC in accordance with DIN EN 50518 / VdS 3138
Police (hold-up/intruder alarm system with direct connection)	Hold-up alarms and selected intruder alarms	ÜEA Guideline, usually Grade 3 or 4, application and acceptance; varies greatly by region
Fire service (via concession holder)	Fire alarms from fire alarm systems required under building law	DIN 14675, fire detection and alarm concept, connection requirements of the fire service, key depot

Fire alarm systems: fire service first, ARC as a supplement

Fire alarms from fire alarm systems required under building law are routed via the transmission device to the alarm transmission network of the local concession holder and go directly to the fire service. Before installation, a fire detection and alarm concept in accordance with DIN 14675 must be agreed with the fire service. Following a decision by the German Federal Cartel Office, the concession may now only cover the receiving equipment at the fire service; the transmission device and the transmission path can be chosen freely on the open market.

A private alarm receiving centre can additionally handle fault and status messages and, in the event of a fire, organise keys, guidance for the fire service and follow-up care – but it does not replace the connection to the fire service.

2.4 Alarm transmission in accordance with DIN EN 50136

The transmission path is the invisible link in the security chain: if it fails unnoticed, even the best system is ineffective. DIN EN 50136-1 distinguishes between single-path transmission (Single Path, SP 1 to SP 6) and dual-path transmission (Dual Path, DP 1 to DP 4). The higher the category, the shorter the supervision intervals and the faster a failure is detected.

Category	Principle	Typical application
SP 1 – SP 3	one transmission path, longer supervision intervals	residential premises, small businesses (Grade 2)
SP 4 – SP 6	one transmission path with close supervision	commercial premises with higher risk
DP 1 – DP 4	primary and backup path, e.g. fixed IP line plus mobile network	Grades 3 and 4, branch networks, critical infrastructure (KRITIS)
BMA to the fire service	at least SP 6 or DP 3	per DIN 14675 / connection requirements

2.5 Fast fault detection

Older dial-up connections need 10 to 15 seconds to establish a connection. Modern, permanently supervised IP connections detect failure or tampering of the control panel or the transmission device considerably faster; according to the guidance issued by VdS and BHE, the alarm receiving centre should be informed within 180 seconds at the latest. Existing systems should be upgraded to this standard.

2G switch-off: check existing systems now

Telekom intends to switch off its 2G network by 30 June 2028, Vodafone in September 2028 and Telefónica by the end of 2028. Vodafone will keep 2G coverage running for critical applications such as older alarm systems until the end of 2030. Alarm transmission devices whose backup path only supports GSM will then lose their second path – often unnoticed until an emergency occurs.

Recommendation: Take stock of existing systems, plan transmission paths based on LTE/5G and IP, and combine the upgrade with maintenance that is due anyway. The 3G network was already switched off in 2021.

Upgrade instead of replacement

When the transmission path is changed, the intruder alarm system rarely needs to be replaced completely. Replacing the transmission device or adding a supplementary module is often sufficient. SecuConCept first checks whether existing systems can continue to be used – this saves costs and resources and reduces the ecological footprint.

Relevance for critical infrastructure (KRITIS)

For operators of critical facilities, Section 13 of the German KRITIS Umbrella Act explicitly lists detection equipment, access controls and defined alarm procedures as resilience measures. Alarm monitoring, alarm plan, intervention and prevention are therefore part of the statutory evidence. Details can be found in the SecuConCept manual "Video Surveillance & Video Monitoring for KRITIS-Relevant Facilities".

DIN EN 50518 · DIN 77200-1 · ALARM PLAN · ON-SITE RESPONSE

03 Alarm Receiving Centre and Alarm Response

All alarms converge in the alarm receiving centre (ARC). It assesses, decides and alerts – around the clock, following an alarm plan agreed with the client.

3.1 Alarm handling procedure

1	**Receipt**	The alarm, including site, detector group and time stamp, is received by the ARC and acknowledged.
2	**Assessment**	An operator checks the alarm type, the event history and, where available, video or audio verification.
3	**Call-back / code word**	Contact with the site or with persons authorised for call-back; the agreed code word is requested.
4	**Alerting**	Intervention service, police or fire service according to the alarm plan; contact persons are informed in parallel.
5	**Support**	Guidance of the response officer, review of the situation, additional alerting if required.
6	**Completion**	Log, deployment report, restoration of the armed state, notification of the client.

3.2 Alarm types and response

Alarm	Typical response of the ARC
Intruder alarm	Verification, alarm response, immediate police alert if there are signs of an offence
Hold-up / silent alarm	no call-back to the site, immediate police alert
Tampering / line fault	call-back, technical service, alarm response in case of suspicion
Technical alarm	contact person or on-call service according to the alarm plan, specialist contractor if required
Arming monitoring	system not armed at the agreed time: call-back, on-site check if required
Disarming outside the agreed hours	code word check, alarm response in the event of a discrepancy

3.3 Quality criteria for an alarm receiving centre

- Certification as an alarm receiving centre in accordance with **DIN EN 50518**, ideally with VdS approval in accordance with **VdS 3138**
- Redundant technology, emergency power, permanent staffing and a documented fallback solution
- Trained staff holding a licence and qualification in accordance with **§ 34a GewO** (German Trade Regulation Act)
- Data processing agreement in accordance with Art. 28 GDPR and traceable logging
- Monthly reporting: alarms, response times, false alarm rate, availability

The alarm plan – the most important document

For each alarm type, the alarm plan defines who is informed in which order, which measures the alarm receiving centre takes, which code word applies and where keys are held. It is approved by the client and updated whenever staff or telephone numbers change. An outdated alarm plan is the most common cause of delayed responses.

3.4 Alarm response in accordance with DIN 77200-1

DIN 77200-1 (current edition 2022-10) sets out minimum requirements for security service providers. It distinguishes between stationary services such as alarm duty and mobile services such as patrol, inspection and intervention services. The intervention service comprises agreed measures in response to a specific, non-regular event within a defined period. The response officer is the extended arm of the ARC; every alarm response must be treated as a potentially genuine alarm.

3.5 On-site procedure

1	**Travel to site**	Confirmation of the assignment to the ARC, travel to the site in compliance with road traffic regulations.
2	**Approach**	Personal safety first, external check, identifying traces of evidence without destroying them.
3	**Situation assessment**	If there are signs of offenders inside the premises: do not enter, request the police, keep the premises under observation.
4	**Internal check**	Only if the situation is inconspicuous: take the keys, walk through the premises, establish the cause.
5	**Securing**	Emergency closure, reset and re-arm the system, guard the premises until the damage is repaired if necessary.
6	**Report**	Deployment report with times, findings and photos to the ARC and the client.

3.6 Rights and limits of the response officer

Private security staff have no sovereign powers. They act on the basis of the domiciliary rights (Hausrecht) delegated by the client and the so-called everyman's rights:

- Self-defence and defence of others (§ 32 StGB, German Criminal Code) and justifying necessity (§ 34 StGB)
- Provisional arrest of an offender caught in the act (§ 127 (1) StPO, German Code of Criminal Procedure) – to be interpreted narrowly, proportionate means only
- Defence of possession and self-help under §§ 859, 229 BGB (German Civil Code)
- Enforcement of domiciliary rights, e.g. ordering persons to leave and issuing bans from the premises on behalf of the client

Domiciliary rights and rights of way – what applies during deployment

Domiciliary rights (Hausrecht): They belong to the owner or occupier and derive from ownership and possession (§§ 858 ff., 903, 1004 BGB). The security service may only exercise them if the client delegates them – preferably in writing, with a clear description of the premises and of the powers conferred (e.g. issuing bans from the premises, directing persons to leave the site). Anyone who stays despite being told to leave may commit trespass (§ 123 StGB); the offence is only prosecuted upon a criminal complaint, which the entitled party must file.

Rights of way under civil law: If access to the site crosses third-party land – for example in business parks, rented properties or industrial estates with several users – the response officer needs a legally secured right of access, e.g. under an easement (§ 1018 BGB), the lease or an agreement with the landowner. The security service must not restrict the rights of third parties (neighbours, co-users); domiciliary rights end at the boundary of the client's property.

Rights of way in road traffic: Private security services have no special or priority rights under §§ 35, 38 StVO (German Road Traffic Regulations) – no blue lights, no siren, no exemptions from speed limits. The response time must therefore be agreed realistically, based on distance and traffic conditions.

In practice: The delegation of domiciliary rights, access and locking authorisations (barriers, gates, codes) and the contact persons of landowners belong in the alarm plan – in writing.

3.7 Key and access management

- Keys held in the certified key safe of the intervention station or in a key depot close to the site
- Sealed, coded key pouches without the site address; removal and return are logged
- Regular functional checks of keys and codes, immediate notification of lock changes

CLIENT · EMPLOYEES · TRAINING · AVOIDING FALSE ALARMS

04 Client Cooperation

Even the best alarm receiving centre can only respond as well as the information it receives. A large proportion of all false alarms and delayed deployments has organisational causes within the premises – and can be avoided through clearly defined cooperation.

4.1 The client's duties to cooperate

Cooperation	Why it matters
Approve the alarm plan and keep it up to date	Incorrect or outdated numbers delay every response
Name at least two reachable persons authorised for call-back	On-site decisions require a responsible person
Hand over keys, codes and access authorisations	Without access, the intervention ends at the door
Delegate domiciliary rights in writing	Legal certainty for the response officer's measures
Report changes to the premises (conversion, change of tenants, storage)	Detectors may become obstructed or need realignment
Register maintenance and inspection work in advance	Avoids false alarms and unnecessary deployments
Announce deviating working hours and special opening times	Otherwise, disarming events are treated as suspicious incidents
Commission maintenance in accordance with DIN VDE 0833	Operator's duty, often an insurance requirement
Review deployment reports and have defects remedied	Recurring causes can only be eliminated this way

4.2 Employee cooperation

Employees arm and disarm the system, open doors and windows and are often the first on site. They therefore need brief, regularly repeated training:

- **Arming:** close windows, doors and gates first, clear detection areas, do not place objects in front of detectors
- **Codes and code word:** do not pass on personal codes; know the code word that the ARC requests during call-back
- **Report operating errors immediately:** anyone who triggers an alarm by mistake calls the ARC without delay – this saves a deployment
- **Hold-up and emergency situations:** know and trigger the silent alarm, do not endanger yourself, do not negotiate with offenders
- **New employees:** instruction before keys or codes are first issued; delete the codes of departed staff immediately

4.3 Common causes of false alarms and countermeasures

Cause	Countermeasure
Operating errors when arming or disarming	Training, blocking lock or forced-arming interlock, clear operating instructions
Windows, doors or gates open during arming	Closure monitoring, checklist at the exit
Animals, warm air from heating, balloons, decorations	Have detector selection and alignment reviewed
Construction work, dust, humidity	Report work in advance, have detectors covered, check after completion
Outdated or dirty detectors	Maintenance in accordance with DIN VDE 0833, replacement instead of a permanent makeshift

Insurance: take policyholder obligations seriously

Many commercial insurance policies stipulate the presence and arming of an intruder alarm system as a policyholder obligation. If this obligation is breached intentionally or through gross negligence – for example because the system was not armed or not maintained – the insurer may reduce its benefits or refuse them entirely under § 28 VVG (German Insurance Contract Act). The arming logs of the alarm receiving centre are important evidence in the event of a claim.

Data protection and co-determination

Alarm plans contain names and telephone numbers; arming logs show who entered or left the premises and when. Employees must be informed in accordance with Art. 13 GDPR. If the data allows conclusions to be drawn about behaviour or performance, an existing works council has a right of co-determination (§ 87 (1) No. 6 BetrVG, German Works Constitution Act) – a brief works agreement creates clarity.

IMPEDE · DETECT · ORGANISE

05 Preventive Security

The best alarm is the one that is never triggered. Preventive security combines mechanical resistance, organisational rules and visible presence – and is what makes detection technology and intervention effective in the first place.

5.1 Principle: mechanics, electronics, organisation

Police crime prevention advice follows the principle that mechanical security measures delay the offender while electronic detection technology discovers them. An offence is only prevented – rather than merely reported – when the resistance lasts longer than alerting and intervention take. The police crime prevention advisory centres provide free, manufacturer-neutral advice; SecuConCept complements this with a site-specific overall concept covering alarm monitoring, intervention and prevention from a single source.

Resistance class, DIN EN 1627	Offender type and approach	Typical application
RC 2	opportunist offenders using simple tools	residential premises, offices, side entrances
RC 3	offenders using additional tools, e.g. crowbars	commercial premises, warehouses, rear sides of branches
RC 4 – RC 6	experienced offenders using power tools	high-value storage, equipment rooms, special facilities

5.2 Building blocks of prevention

Building block	Content
Vulnerability analysis	Site inspection by day and night, offender's perspective, assessment of access points, lighting, lines of sight
Security concept	Protection goals, mix of mechanical, technical and organisational measures, responsibilities
Patrol and inspection service	Irregular checks at varying times, visible presence, defect reports
Locking and opening service	Controlled locking, arming and logging in the evening
Access and key management	Authorisations on a need-to-have basis, loss procedure, regular clean-up
Lighting and grounds	Motion-activated lighting, clear lines of sight, no climbing aids on façades
Emergency and crisis management	Alarm and emergency plans, contact persons, exercises, follow-up
Fire prevention	Fire safety regulations, fire safety assistants, fire watches during hot work

§ 34A GEWO · FALSE ALARM FEES · GDPR

06 Law, Liability and Data Protection

Alarm monitoring and alarm response touch on trade, police, civil and data protection law. These points should be regulated by contract.

6.1 Trade law

- Security companies require a licence under § 34a GewO (German Trade Regulation Act); their employees are recorded in the national guarding register and, depending on their duties, require instruction or an expert knowledge examination before the Chamber of Commerce and Industry (IHK).
- The Security Industry Ordinance (BewachV) governs, among other things, liability insurance, service instructions and the duty to carry identification.

6.2 False alarms and fees

Whether and in what amount police or fire services charge fees for false alarms is governed by the law of the federal state or the municipal fee schedule. The German Federal Administrative Court considers reasonable fees for a police deployment triggered by an alarm system to be permissible. The Administrative Court of Neustadt confirmed 120 € for an unjustified alarm call-out triggered by an intruder alarm system; an alarm is deemed unjustified if the police cannot establish a cause. Fire services usually charge for false alarms on the basis of time, personnel and vehicles. In Baden-Württemberg, around 29,500 fire service deployments were classified as false alarms within a single year.

6.3 Liability and contract

- Specify in writing the scope of services, response time, key liability, liability limits and third-party damage in the event of forced entry
- The alarm receiving centre is responsible for alarm handling and alerting, not for the functioning of the system on the premises
- Request proof of the service provider's business liability and key insurance

6.4 Data protection

Topic	Implementation
Roles	The ARC and the intervention service generally act as processors: data processing agreement in accordance with Art. 28 GDPR
Data scope	Only the necessary contact details in the alarm plan; codes and code words stored separately and protected
Retention periods	Delete alarm logs and deployment reports after the agreed period; exceptions in the event of damage and legal proceedings
Video, audio and technology	Verification only for alarm assessment; encrypted transmission, role-based and logged access

REFERENCE VALUES · INVESTMENT · OPERATION

07 Cost Examples and Cost-Effectiveness

The examples show typical cost structures for budget planning and comparison. All figures net, market level 2026; actual costs depend on the size of the site, grade, transmission path, distance to the intervention station and scope of services.

Example A – Warehouse and office building, 1,500 m², intruder alarm system Grade 3 / VdS Class B

Item	Quantity	Unit price	Total
Vulnerability analysis and planning	flat rate		1,200 €
Intruder alarm control panel with operating unit	1	2,400 €	2,400 €
Motion detectors	24	95 €	2,280 €
Opening and closure monitoring	12	65 €	780 €
External sounder with strobe light	1	450 €	450 €
Transmission device IP/LTE, dual path	1	650 €	650 €
Installation and commissioning	flat rate		3,800 €
Acceptance and installation certificate	flat rate		450 €
Total investment (net)			**12,010 €**

Annual running costs	Calculation	Amount
ARC monitoring incl. arming supervision	49 € × 12 months	588.00 €
Key holding	15 € × 12 months	180.00 €
Mobile network tariff for the backup path	9.90 € × 12 months	118.80 €
Maintenance in accordance with DIN VDE 0833	2 × 290 €	580.00 €
Alarm response (assumption: 6 deployments)	6 × 95 €	570.00 €
Depreciation of the investment (10 years, straight-line)	12,010 € ÷ 10	1,201.00 €
Total annual costs		**3,237.80 €**

This corresponds to around 270 € per month, or just under 9 € per day, for protecting the entire premises.

Example B – What false alarms cost and what prevention saves

Item	Before (12 false alarms)	After (3 false alarms)
Alarm response at 95 € each	1,140.00 €	285.00 €
Police fee at 120 € each (assumption: 4 and 1 case(s))	480.00 €	120.00 €
Internal effort (1.5 h at 45 € per false alarm)	810.00 €	202.50 €
Costs per year	**2,430.00 €**	**607.50 €**

One-off cost of employee training and detector optimisation (assumption): 750 €. Savings in the first year: 1,822.50 € − 750 € = 1,072.50 €; from the second year onwards, 1,822.50 € per year.

Example C – Preventive mobile patrols complementing the alarm monitoring

Item	Calculation	Amount
Night patrol on every day of the year	365 × 22 €	8,030 €
Additional daytime patrol at weekends	104 × 22 €	2,288 €
Patrol service per year		**10,318 €**

Advocatus Diaboli: a cheap connection is paid for dearly

Low monthly prices for alarm monitoring say little about the service behind them. What matters are the certification of the alarm receiving centre, the agreed response time, the qualification of the response staff, key liability and reporting. A quotation without a binding response time or without proof of DIN EN 50518 certification is not comparable – and, in the event of a claim, often not acceptable to insurers either.

FROM ANALYSIS TO ROUTINE OPERATION

08 Checklist for Clients

The checklist is suitable for internal coordination, tender procedures and evidence provided to insurers, supervisory authorities and auditors.

Phase 1 – Analysis	
☐	Define protection goals, assets and risks for each site; check insurance requirements
☐	Vulnerability analysis with site inspections by day and night
☐	Record existing systems: grade/class, age, transmission path, 2G dependency
☐	Clarify connection targets: ARC, police, fire service via the concession holder

Phase 2 – Concept and award	
☐	Security concept combining mechanical protection, detection technology, organisation and intervention
☐	Service specification including response time, reporting and liability
☐	Request evidence: DIN EN 50518 / VdS 3138, § 34a GewO, insurance policies, data processing agreement
☐	Clarify access and rights of way across third-party land

Phase 3 – Commissioning	
☐	Define and approve the alarm plan, the code word and the persons authorised for call-back
☐	Hand over keys, codes and access authorisations with documented records
☐	Delegate domiciliary rights in writing
☐	Train employees; provide data protection information and, where applicable, a works agreement
☐	Carry out a test alarm across all transmission paths

Phase 4 – Routine operation	
☐	Update the alarm plan after every change; review it at least once a year
☐	Maintenance in accordance with DIN VDE 0833 and checks of the transmission paths
☐	Evaluate the monthly reports; eliminate recurring false alarms
☐	Repeat the training annually and for new employees

SHORT, RELIABLE ANSWERS

09 Frequently Asked Questions (FAQ)

What is the difference between alarm monitoring and alarm response?

The alarm monitoring connection links the hazard alert system to a permanently staffed alarm receiving centre that assesses incoming alarms. Alarm response is the on-site deployment that the ARC initiates in accordance with the alarm plan.

Can I connect my fire alarm system to a private alarm receiving centre?

Fire alarm systems required under building law must be connected to the fire service via the concession holder. A private ARC can additionally monitor faults and organise keys and guidance for the fire service during a deployment.

How quickly will the response officer be on site?

That depends on distance, traffic conditions and the contract. Security services have no special privileges in road traffic; reputable providers agree a realistic, measurable response time for each site.

May the response officer detain an offender?

Only within the scope of the everyman's rights, in particular the provisional arrest of an offender caught in the act under § 127 StPO, and using proportionate means. Personal safety and alerting the police take priority.

Who pays in the event of a false alarm?

Deployments of the intervention service are billed according to the contract. Fees charged by the police or fire service are governed by the law of the federal state or municipal bylaws and are generally payable by the operator of the system.

Will my alarm system still work after the 2G switch-off?

If the transmission device uses GSM only, it will no longer work reliably. Have the transmission path checked now – replacing a module or device is often sufficient.

What cooperation is expected from us?

An up-to-date alarm plan, reachable contact persons, handed-over keys and codes, domiciliary rights delegated in writing, maintenance work registered in advance, and trained employees.

Do we need a new alarm system for the monitoring connection?

Usually not. Existing systems can often be connected using a new transmission device, provided that their grade and condition match the risk.

SECURITY · CONSULTING · CONCEPTION

10 Your Partner for Alarm Monitoring and Intervention

SecuConCept combines manufacturer-independent consulting, security concept design and operational implementation from a single source – throughout Germany, personally coordinated.

Consulting

Vulnerability analysis, review of existing systems and transmission paths, tender support

Conception

Security and alarm concepts, alarm plans, training concepts for employees

Security

Alarm monitoring, alarm response, remote gatehouse, mobile patrol, locking and site services, fire watches

Why SecuConCept?

- **SecuNET by SecuConCept:** more than 350 specialised security companies throughout Germany – intervention with regional local knowledge and uniform quality requirements.
- **One contractual partner:** Even when SecuNET partners intervene on site, SecuConCept remains your contractual partner and coordinator.
- **Certified, redundant alarm receiving centre** in accordance with DIN EN 50518 / VdS – also for private customers and small commercial premises.
- **Manufacturer-independent and economical:** no commissions from manufacturers, "upgrade instead of replacement" for existing systems, up to 15 % discount for framework agreement customers.

Specialist portals and brands

CCTV-SECURITY.DE
VIDEOTÜRME | ALARMZENTRALE | ALARMVERFOLGUNG | REALISIERUNG
by SecuConCept

CCTV-Security.de by SecuConCept – specialist portal for video towers, alarm centre, alarm response and implementation.

SecuFokus®
SICHERHEIT GEMEINSAM STEUERN.
BY SECUCONCEPT

SecuFokus by SecuConCept – Managing Security Together.
Specialist information and tools for operators, partners and service providers.

FREE INITIAL CONSULTATION

Alarm monitoring check for your sites

Existing systems, transmission paths, alarm plan and response times – in one structured meeting with a clear recommendation for action.

0800 666 000 4 (nationwide, Germany) · 0221 954 917 52 (Cologne)

vertrieb@secuconcept.de · www.secuconcept.de

SecuConCept · Owner: Torsten Bentlage · Adolf-Grimme-Allee 3 · 50829 Köln

FOR REFERENCE

11 Sources, Standards and Legal Status

Standards and guidelines

- DIN VDE 0833-1/-2/-3 – hazard alert systems for fire, intrusion and hold-up
- DIN EN 50131 (series) – alarm systems, intruder and hold-up alarm systems; VdS 2311 – planning and installation of intruder alarm systems
- DIN EN 50136-1/-2 – alarm transmission systems and equipment
- DIN EN 50518 – alarm receiving centre; VdS 3138 – emergency call and service control centres (NSL)
- DIN 77200-1:2022-10 – security services, general requirements
- DIN 14675 – fire alarm systems, design and operation; DIN EN 54 – fire detection and alarm systems
- DIN EN 1627 – burglary resistance of doors, windows and closures
- Guideline for hold-up and intruder alarm systems with connection to the police (ÜEA Guideline)

Legal foundations

- § 34a GewO (German Trade Regulation Act), Security Industry Ordinance (BewachV)
- §§ 32, 34, 123 StGB (German Criminal Code); § 127 StPO (Code of Criminal Procedure); §§ 229, 858 ff., 903, 917, 1004, 1018 BGB (German Civil Code); §§ 35, 38 StVO (Road Traffic Regulations)
- § 28 Insurance Contract Act (VVG); § 87 Works Constitution Act (BetrVG)
- GDPR, in particular Art. 13, 28, 32; § 13 KRITIS Umbrella Act
- Federal Administrative Court (BVerwG), judgment of 23 August 1991 – 8 C 37.90 (fees for police deployments following alarm activation)

Further sources

- Federal Network Agency and network operators: information on the switch-off of the 2G networks (as of 2026)
- BHE / VdS: guidance on the defeat of intruder alarm control panels and transmission devices
- Connection requirements of the fire services for fire alarm systems; guidance of the Federal Cartel Office on the award of concessions

Legal status and liability: Research status November 2026. Connection requirements, fees and police guidelines differ by federal state and municipality. This manual does not constitute legal advice. Cost figures are non-binding reference values (net) based on typical project assumptions.

© 2026 SecuConCept · Owner: Torsten Bentlage · Distribution in unchanged form is expressly welcome.